ดร.ปัญญา เปรมปรีดิ์

ความชั่วร้ายที่แฝงกายในอินเทอร์เน็ต

จริงหรือ ที่ในอินเทอร์เน็ต
มีความชั่วร้ายแฝงกายอยู่

ผมได้อ่านบทความในหนังสือพิมพ์ฉบับหนึ่งหัวเรื่องของเขาคือ "What the "Net" can do for you" ซึ่งเป็นการแนะนำให้รู้ว่าเครือข่าย "Internet" สามารถจะทำอะไรให้ท่านได้บ้าง บทความดังกล่าวเสนอมาให้รูปแบบที่เข้าใจได้ง่าย ๆ เสนอแบบตรงไปตรงมา แต่ผมคิดว่ามันยังไม่ครบถ้วน ผมก็เลยอยากจะให้มองทางด้านลบดูบ้าง

สิ่งแรกที่ผมอยากให้ท่านระมัดระวังก็คือ **ความปลอดภัยของข้อมูลนั้นยังมีน้อย และเราอาจเข้าใจผิดกันได้ง่ายมาก** กล่าวคือ ผู้ขายซอฟต์แวร์และผู้ขายบริการอินเทอร์เน็ตมักจะบอกว่าเขามีระบบที่จะช่วยในการเข้ารหัสข้อมูลให้เราได้ แล้วเขาก็จะยกตัวอย่างเรื่องการส่งหมายเลขของบัตรเครดิตของท่านให้ฟัง สิ่งที่เขาอธิบายนั้นจะเข้าใจได้ไม่ยาก คือเขาจะบอกว่ามันมีขั้นตอนเพียง 3 ขั้นตอน คือ

1. โปรแกรมในเครื่องของเราจะนำเอาหมายเลขบัตรของเราไปคำนวณตามสูตรของการเข้ารหัส ซึ่งจะให้ผลเป็นตัวเลขหรือข้อมูลที่คนอื่นไม่สามารถจะตีความออกมาได้

2. ตัวเลขหรือข้อมูลที่เข้ารหัสแล้วนั้นจะถูกส่งผ่านเครือข่ายไปสู่บริษัทผู้ขายสินค้า

3. เครื่องของบริษัทผู้ขายสินค้าจะนำเอาตัวเลขหรือข้อมูลที่เข้ารหัสแล้วนั้นไปคำนวณตามสูตรในการถอดรหัส ผลที่ได้จะเป็นหมายเลขบัตรของเรา ซึ่งเขาสามารถใช้ทำเป็นสลิปเพื่อส่งไปตัดบัญชีที่ธนาคารที่เราไปทำบัตรเครดิตเอาไว้

และเขาจะย้ำนักย้ำหนาว่าบุคคลที่ 3 ไม่มีหนทางทราบหมายเลขบัตรเครดิตของเราได้เลย ใครที่ดักจับข้อมูลในขั้นตอนที่ 2 ไปได้นั้นจะต้องใช้เวลาหลายพันปีในการแกะหากุญแจในการถอดรหัสและเขาจะบอกเพิ่มเติมมาว่า ราคาของโปรแกรมที่จะใช้ในการเข้ารหัสและถอดรหัสนั้นจะมีแผก ๆ แตกต่างกันไป กล่าวคือ "ถ้าจะให้ป้องกันได้ดีก็จะมีราคาแพงหน่อย"

สิ่งที่ทำให้เราเข้าใจกันผิดได้นั้นมี 2 แห่ง แห่งแรกก็คือ เขาพูดแต่เพียงว่า บุคคลที่ 3 นั้นถึงแม้จะแอบดักจับข้อมูลจากเครือข่ายไปได้ก็ต้องใช้เวลามากมายในการแกะหากุญแจในการถอดรหัส **เมื่อได้กุญแจแล้วจึงจะสามารถรู้หมายเลขบัตรเครดิตของเรา แล้วจึงจะโกงเราได้** แต่ในความเป็นจริงนั้นผู้ร้ายอาจไม่ต้องเสียเวลาแกะหากุญแจในการถอดรหัสเลยก็ได้ เขาสามารถใช้เจ้าข้อมูลที่เข้ารหัสแล้วอันนั้นเพื่อโกงท่านได้ ถ้าเราใช้การเข้ารหัสที่ไม่ถูกวิธี เรื่องนี้เดี๋ยวผมจะอธิบายเพิ่มเติมให้ฟัง ข้อที่จะทำให้พวกเราเข้าใจผิดเป็นแห่งที่ 2 ก็คือ คำอธิบายข้างบนนั้นเป็นการชี้นำไปว่าโปรแกรมที่ดี ที่มีราคาแพงนั้นจะทำให้ผู้ร้ายใช้เวลาในการแกะหากุญแจในการถอดรหัสเป็นเวลายาวนานขึ้น **ส่วนโปรแกรมที่มีราคาถูก ๆ หรือที่ให้เราใช้ได้ฟรี ๆ นั้นก็จะมีความสามารถในการป้องกันความลับได้คล้ายกัน แต่ใช้เวลาในการแกะหากุญแจไม่ยาวนานนัก**

รายละเอียดของปัญหา

ผมจะขอเข้ามาดูรายละเอียดของปัญหาประเภทแรกเสียก่อน กล่าวคือ มีคนเชื่อกันมากว่าผู้ร้ายนั้นดักจับข้อมูลจากเครือข่ายไปแล้วก็ทำประโยชน์อะไรไม่ได้ เรื่องนี้เป็นจริงแต่ในเรื่องของการส่งข้อความหรือคำพูดต่าง ๆ ยกตัวอย่างเช่น ทหารจากแนวรบด้านหน้าอาจต้องการส่งข่าวสารเพื่อบอกสถานการณ์ให้แนวหลังทราบ หรืออาจต้องการขอกำลังเพิ่มเติม ข่าวสารประเภทนี้เป็นข้อความ ซึ่งถ้าดักจับไปได้ก็จะต้องหาทางแกะหากุญแจและทำการถอดรหัสออกมาเสียก่อน จึงจะใช้ประโยชน์ได้ แต่ถ้าเป็นการส่งคำสั่งตามตามรูปแบบที่แน่นอน และผู้ร้ายรู้ว่าภายในนั้นบรรจุคำสั่งอะไรเอาไว้ พวกเขาก็อาจใช้ประโยชน์ได้ ยกตัวอย่างเช่น ผู้ร้ายเอาเงินสดจำนวนหนึ่งไปยังสาขา A แล้วขอให้สาขานั้นทำการโอนเข้าบัญชีของเขาที่สาขา B เมื่อส่งมอบเงินไปเรียบร้อยแล้วก็ให้เพื่อนคอยดักจับสัญญาณการสั่งโอนเงินดังกล่าวผ่านระบบสายโทรศัพท์ ถ้าวันนั้นหรือในช่วงเวลานั้นไม่มีการสั่งโอนโดยลูกค้ารายอื่นเลย เขาก็พอจะเชื่อได้ว่าสัญญาณที่จับได้นั้นเป็นคำสั่งโอนเงินเข้าบัญชีของตน เมื่อทราบอย่างนี้แล้วก็สามารถจะหลอกธนาคารได้ทั้งนี้โดยการส่งสัญญาณไปอีกในวันหรือเวลาอื่น อย่างนี้เราเรียกว่าการ "ทำซ้ำ" ของคำสั่ง ในกรณีนี้ถ้าธนาคารไม่มีระบบป้องกันตัว สาขา B ก็อาจเข้าใจว่าเป็นการสั่งโอนเป็นครั้งที่ 2 แล้วก็จะดำเนินการเอาเงินเข้าบัญชีให้อีก การทำซ้ำนี้อาจทำกี่ครั้งก็ได้ เมื่อเป็นที่พอใจแล้วก็ไปขอเบิกเงินจากบัญชีที่สาขา B ตามจำนวนรวมที่สั่งโอนมา

วิธีการป้องกันตัวของธนาคารนั้นมี 2 วิธี วิธีแรกคือ ออกเป็นเงื่อนไขว่าโอนเงินข้ามสาขานั้นจะยังไม่ให้ถอนในวันเดียวกัน ด้วยวิธีนี้ธนาคารจะมีเวลาในการสอบยันกันระหว่างสาขา ธุรกรรมแบบนี้เป็นธุรกรรมที่ต้องลงบัญชีเป็นเจ้าหนี้และลูกหนี้ระหว่างกันของสาขา ซึ่งรายการเหล่านี้จะถูกส่งเข้าสู่สำนักงานใหญ่ในตอนกลางคืน และสำนักงานใหญ่จะต้องสอบยันให้สาขาต่าง ๆ การแอบทำซ้ำจะเกิดการเขย่งระหว่างสาขาทั้งสอง ธนาคารก็สามารถจะระงับการจ่ายเงินได้ แต่การสอบยันเหล่านี้บางธนาคารทำไม่ทันในวันเดียว ในกรณีนั้นก็จะต้องใช้วิธีการที่ 2 วิธีการที่ 2 คือ ทุกครั้งที่จะส่งคำสั่งการโอนเงินนั้นเขาจะเอาคำสั่งโอน วันเวลา และหมายเลขลำดับที่ของการสั่งโอนบรรจุเป็นข้อความร่วม และจะต้องเข้ารหัสข้อความทั้งหมดในคราวเดียวกัน ผลที่ได้จะเป็นข้อมูลที่ยาวกว่าเดิมมาก แล้วจึงจะส่งผ่านสายสื่อสารไป เมื่อไปถึงสาขา B แล้วก็ต้องถอดรหัสทั้งยวง **และก่อนที่จะทำการโอนเงินเข้าบัญชีจริง ๆ ก็ต้องเช็ค "วันเวลาและหมายเลขลำดับที่ของการสั่งโอน" ด้วย ถ้าเป็นตัวเลขที่ซ้ำกันก็ต้องสอบถามสาขา** A ด้วยวิธีนี้เขาจึงจะสามารถจับความผิดปกติได้ **ซึ่งเรื่องอย่างนี้เครือข่ายอินเทอร์เน็ตทำให้ไม่ได้** เท่าที่ผมเห็นมา โปรแกรมที่ใช้ในการเข้ารหัสเพื่อส่งหมายเลขบัตรเครดิตไปยังผู้ขายสินค้าจะไม่มีการบอกวันเวลาหรือหมายเลขลำดับที่ของรายการ ตัวคำสั่งซื้อและบ้านเลขที่ที่จะส่งสินค้าไปนั้นไม่อยู่ในขบวนการเข้ารหัส ดังนั้นผู้ร้ายที่ดักจับข้อมูลหมายเลขบัตรเครดิตที่เข้ารหัสแล้วนั้นสามารถนำไปติดต่อและสั่งเป็นคำสั่งซื้อสินค้าได้อีก สินค้าจะถูกส่งไปยังบ้านเลขที่ใหม่ (=บ้านผู้ร้าย) แต่การหักบัญชียังหักจากบัตรเครดิตใบเดิม ปัญหานี้ถ้าคิดกันให้ละเอียดก็จะพบว่า ถึงแม้จะมีการปรับปรุงให้มีการบอกวันเวลาและหมายเลขลำดับที่ และให้มีการเข้ารหัสพร้อม ๆ กับหมายเลขบัตรเครดิต ซึ่งจะทำให้ผู้ร้ายไม่สามารถแก้บ้านเลขที่ แต่ผู้ร้ายก็ยังสามารถกลั่นแกล้งท่านได้ ทั้งนี้โดยส่งซ้ำเป็นร้อย ๆ ครั้ง แล้วท่านก็จะได้รับสินค้าเกินความต้องการ ผมเชื่อว่าเมื่อไหร่ที่พิซซ่าฮัทเปิดบริการสั่งผ่านเครือข่ายก็จะต้องมีคนที่ตื่นเช้าขึ้นมาแล้วพบว่ามีกล่องพิซซ่ากองท่วมหัวอยู่หน้าบ้าน ทั้งนี้เพราะเขาไปสั่งพิซซ่ามากินกันสนุกสนานในคืนวันก่อนและทำเสียงดังจนเกินกว่าเหตุ

ขอผ่านมาถึงเรื่องของความเข้าใจผิดกันในรูปแบบที่ 2 ความเข้าใจผิดก็คือ คนที่ไม่เข้าใจเรื่องคอมพิวเตอร์ดีพอก็จะคิดเอาเองว่าโปรแกรมเพื่อเข้ารหัสนั้นเป็นสิ่งที่ทำขึ้นเป็นพิเศษ ตัวที่ราคาแพงจะมีความยุ่งยากและซับซ้อนมากกว่าตัวราคาถูก การเลือกโปรแกรมจึงเป็นเรื่องของวงเงินและความเสี่ยง เช่น เมื่อซื้อตำรา 1 เล่ม ราคา 500 บาท ก็เลือกใช้โปรแกรมที่ไม่แพงนัก แต่ถ้าสั่งซื้อเครื่องเพชรหรือนาฬิกาหรู ๆ ในราคา 500,000-600,000 บาท ก็ต้องใช้โปรแกรมที่ดีกว่าหน่อย

จริง ๆ แล้วในหลักการของการเข้ารหัสและถอดรหัสนั้น โปรแกรมที่ใช้งานจะเป็นโปรแกรมที่ขายอย่างเปิดเผย ความยากง่ายของการขโมยความลับไม่ได้อยู่ที่การปิดลับหรือเก็บงำโปรแกรมเอาไว้ โปรแกรมที่เขาวางขายจะเป็นที่รู้กันหมด และถ้ามาจากต้นตอเดียวกันก็จะเหมือนกันหมด ตัวที่เราต้องเก็บงำและปิดลับคือกุญแจเพื่อเข้ารหัส ความแตกต่างนั้นอยู่ที่เทคนิคการเข้ารหัสและถอดรหัสกับความยาวของตัวกุญแจเข้ารหัส ความยาวของตัวกุญแจเข้ารหัสคือตัวที่จะทำให้ผู้ร้ายต้องใช้เวลาแกะรหัสนานกว่ากัน คือยิ่งยาวยิ่งยาก สำหรับเทคนิคการเข้ารหัสนั้นมี 2-3 วิธีเท่านั้นที่เขาใช้กันจริง ๆ ได้แก่ DES และ RSA แบบ DES นั้นตัวกุญแจเพื่อใช้เข้ารหัสและกุญแจเพื่อถอดรหัสจะเป็นตัวเดียวกัน ตัวโปรแกรมเพื่อเข้ารหัสและเพื่อถอดรหัสก็เป็นโปรแกรมเดียวกัน โปรแกรมนี้มีวิธีการคำนวณง่าย ๆ แต่ทำซ้ำหลายครั้ง มันจึงกินกำลังเครื่องสูง การเข้ารหัสข้อมูลยาว 80 ตัวอักษร และใช้กุญแจที่มีความยาว 56 ตัวอักษร จะใช้เวลาเกือบ 1 วินาที การถอดรหัสก็ใช้เวลาเท่ากัน ด้วยเหตุนี้ผู้ใช้จึงมักจะพยายามใช้เข้ารหัสแต่เฉพาะส่วนที่จำเป็น เช่น การสั่งซื้อสินค้าผ่านเน็ตเวอร์กก็อาจเข้ารหัสแต่เฉพาะตัวหมายเลขบัตรเครดิต การโกงโดยวิธี "ทำซ้ำ" จึงเกิดขึ้นได้ แต่ประเด็นในตอนนี้จะมาอยู่ที่คำถามว่าผู้ขายสินค้าจะส่งกุญแจเพื่อเข้ารหัสไปให้ลูกค้าได้อย่างไร? กุญแจดังกล่าวนี้จะเป็นตัวเลขหรือตัวอักษร ซึ่งยาว 48 ถึง 56 ตัวอักษร กุญแจเข้ารหัสดังกล่าวนี้จะต้องเปลี่ยนใหม่ทุกครั้งที่มีการสั่งซื้อสินค้า การส่งกุญแจครั้งแรกจะเป็น

แบบเข้ารหัสไม่ได้ ทั้งนี้เพราะลูกค้ายังไม่มีอะไรอยู่ในมือเลย นี่เป็นช่องโหว่ที่สำคัญอันหนึ่ง ซึ่งผู้ขายโปรแกรมและผู้ให้บริการเครือข่ายเขาไม่ได้อธิบาย และเขาถือว่าไม่ได้อยู่ในความรับผิดชอบของเขา ยกตัวอย่างเช่น เมื่อท่านตกลงจะซื้อสินค้าแล้วก็จะต้องขอกุญแจจากผู้ขาย กุญแจจะถูกส่งมาทางเครือข่าย ในช่วงตอนนี้ถ้ามีใครดักจับสัญญาณไปก็เป็นปัญหาของท่าน เขาไม่รับผิดชอบ เมื่อท่านเข้ารหัสหมายเลขบัตรเครดิตส่งออกไปก็อาจถูกดักจับอีก ถึงตอนนั้นผู้ร้ายก็สามารถถอดรหัสเพื่อดูหมายเลขบัตรเครดิตของท่านได้ เรื่องนี้ท่านอย่าคิดว่ามันเป็นการรับส่งข้อมูลเป็นระยะสั้น ๆ แล้วจะเสี่ยงน้อย ทั้งนี้เพราะผู้ร้ายไม่ต้องนั่งถ่างตาดูสัญญาณที่ผ่านไปมา เขาใช้วิธีแท็บสายแล้วบันทึกลงจานแม่เหล็กเอาไว้ตลอดวันได้ เมื่อว่างก็ค่อยมาวิเคราะห์ว่าท่านทำอะไรกับเครือข่ายบ้าง เจ้ากุญแจเพื่อเข้ารหัสจึงไม่รอดพ้นสายตาเขาไปได้ อนึ่ง ท่านควรสังเกตว่าระบบ DES นี้ถ้าร้านค้าคิดจะโกงท่าน ท่านจะไม่มีหนทางเถียงเขาได้เลย ทั้งตัวท่านและตัวเขาต่างใช้กุญแจรหัสตัวเดียวกัน เมื่อท่านส่งหมายเลขบัตรเครดิตไปให้เขาแล้ว เขาทำคำสั่งซ้ำอีกกี่ครั้งก็ได้ ท่านสั่งซื้อรองเท้า 1 คู่ก็อาจได้เสื้อเชิ้ต เน็คไท กระเป๋าถือ และอื่น ๆ (เท่าที่เขาอยากจะโล๊ะมาให้) อีก แต่เขาไม่ได้ให้ฟรี เขาหักเงินจากบัญชีไปจนครบ ถ้าท่านอยากจะส่งคืนก็ต้องจ่ายค่าคืนสินค้า ถ้าท่านบอกว่าไม่เคยสั่งซื้อก็ต้องขึ้นศาล ซึ่งท่านไม่มีหนทางสู้คดีได้เลย

ไหน ๆ ก็เขียนมาจนยืดยาวแล้ว ผมก็ขอให้รายละเอียดในระบบแบบ RSA ไปด้วย ระบบนี้ใช้กุญแจในการเข้ารหัสแตกต่างจากกุญแจถอดรหัส โปรแกรมที่ใช้เข้ารหัสกับถอดรหัสก็เป็นคนละโปรแกรม กุญแจเข้ารหัสกับถอดรหัสจะเป็นคู่กัน ผู้ขายสินค้าจะเป็นผู้เก็บกุญแจถอดรหัสเอาไว้ และต้องเก็บเป็นความลับสำหรับกุญแจเพื่อเข้ารหัสนั้นเขาสามารถเปิดเผยได้ โดยทั่ว ๆ ไปก็จะอยู่ในโฮมเพจของเขานั่นแหละ ด้วยวิธีนี้เขาไม่ต้องส่งกุญแจเพื่อเข้ารหัสมา ใคร ๆ ก็เรียกดูได้ แต่เมื่อเรานำมาเข้ารหัสแล้วคนอื่นจะไม่สามารถถอดรหัสได้ ถึงแม้จะมีโปรแกรมเพื่อถอดรหัสก็ทำไม่ได้ ทั้งนี้เพราะต้องใช้กุญแจถอดรหัสซึ่งอยู่ในครอบครองของผู้ขายสินค้าแต่เพียงผู้เดียว ระบบแบบนี้จะให้ความคุ้มครองกับลูกค้าที่ดีกว่า กล่าวคือ มันไม่มีช่องโหว่ในเรื่องการส่งกุญแจเข้ารหัสให้แก่ลูกค้า แต่อย่างไรก็ตามมันก็ยังมีปัญหาในเรื่องการดักจับสัญญาณและส่งซ้ำ และในขณะเดียวกัน การสร้างกุญแจเป็นคู่กันนั้นใช้เทคนิคและเวลาในการสร้าง เจ้าของเทคนิคนี้จึงคิดเงินแพง แถมโปรแกรมที่ใช้เข้ารหัสและถอดรหัสก็ยังกินกำลังเครื่องสูงขึ้นไปอีก เทคนิคนี้จึงขายได้น้อยมาก ผมไม่เชื่อว่าร้านค้าเล็ก ๆ น้อย ๆ ในอินเทอร์เน็ตจะยอมเสียเงินซื้อมาบริการลูกค้า นอกจากนี้แล้ว ในขณะนี้รัฐบาลของท่านคลินตันก็ประกาศห้ามขายโปรแกรมและกุญแจที่มีความยาวในระดับ 56 ไบต์ไปแล้ว เขาให้ขายได้แต่พวกใช้กุญแจสั้น ๆ ซึ่งอาจถูกแกะรหัสได้ในไม่กี่ชั่วโมง มันจึงพอจะสรุปได้ว่า ในขณะนี้ยังมีความเสี่ยงสูงมาก ในตอนนี้ต่อให้เอาพระอินทร์มาพูดผมก็ไม่เชื่อว่ามีความปลอดภัยพอ

จริง ๆ แล้ว The Net นั้นทำอะไร ๆ ไม่ได้อีกหลายอย่าง เช่น เราจะรู้ได้อย่างไรว่าข้อมูลที่ได้มานั้นถูกต้อง ครบถ้วน ไม่ถูกบิดเบือน? เราจะรู้ได้อย่างไรว่าเวบไซท์ที่ติดต่อไปนั้นทำธุรกิจจริง ไม่ได้ตั้งขึ้นมาเพื่อหรอกเอาหมายเลขบัตรเครดิตเราไปใช้? เราจะรู้ได้อย่างไรว่าฐานข้อมูลของเราจะไม่ถูกขโมยไปใช้? เราจะรู้ได้อย่างไรว่าคนที่ติดต่อเข้ามานั้นไม่ใช่มนุษย์บ้ากามหรือเป็นโรคจิต? เราจะรู้ได้อย่างไรว่าเราจะไม่ถูกใช้เป็นสถิติเพื่อการโฆษณาชวนเชื่อต่าง ๆ? และที่ร้ายที่สุดคือ เราจะแน่ใจได้อย่างไรว่า The Net จะไม่เป็นแหล่งแพร่เชื้อไวรัสคอมพิวเตอร์ตัวใหม่ที่สามารถทำลายฐานข้อมูลต่าง ๆ ได้ทั้งโลก? สิ่งเหล่านี้ The Net ช่วยอะไรเราไม่ได้เลย

ผมไม่อยากจะถูกกล่าวหาว่าเป็นคนมองโลกในแง่ร้าย แต่ผมคิดว่า The Net น่าจะเป็นแห่งแรกที่จะถูกโจมตีโดยโปรแกรมเมอร์โรคจิต และถ้าจะให้ The Net ยังอยู่ต่อไปได้ พวกเราก็คงจะต้องช่วยกันระมัดระวังด้วย อย่าเชื่ออะไรง่าย ๆ จนปล่อยให้เกิดความหละหลวมในระบบงาน